Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Claims 1– 21 (cancelled)

22. (currently amended) A method comprising: storing a first secret key on an FPGA chip; causing the FPGA to calculate a message authentication code (MAC) corresponding to a user design; and storing the message authentication code with bitstream information in a nonvolatile memory external to the FPGA chip.

23. (original) The method of claim 22 further comprising: storing copyright messages with the bitstream information; detecting unauthorized alterations to the bitstream using the message authentication code; and preventing bitstreams which have been altered from being used to configure an FPGA.

24. (original) The method of claim 22 further comprising: recording the message authentication code along with corresponding identification information for a product containing the FPGA; and examining the message authentication code stored in the nonvolatile memory of a product containing a pirated FPGA design, which will enable determining the identity of the customer to whom the pirated FPGA was originally supplied using a record of MACs and corresponding product identification.

Claims 25-47 (cancelled)

48. (currently amended) A method comprising: storing a first secret key on an FPGA chip; using the first secret key and a user design to calculate a message authentication code (MAC) corresponding to the user design; and storing the message authentication code with bitstream information in a nonvolatile memory external to the FPGA chip.

49. (previously presented) The method of claim 48 further comprising: storing copyright messages with the bitstream information; detecting unauthorized alterations to the bitstream using the message authentication code; and preventing bitstreams which have been altered from being used to configure an FPGA.

50. (previously presented) The method of claim 48 further comprising: recording the message authentication code along with corresponding identification information for a product containing the FPGA; and examining the message authentication code stored in the nonvolatile memory of a product containing a pirated FPGA design, which will enable determining the identity of the customer to whom the pirated FPGA was originally supplied using a record of MACs and corresponding product identification.